



Europäisches
Patentamt

European
Patent Office

Office européen
des brevets

Bescheinigung

Certificate

Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

03250714.7

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk



Anmeldung Nr:
Application no.: 03250714.7
Demande no:

Anmeldetag:
Date of filing: 04.02.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

STMicroelectronics Limited
1000 Aztec West
Almondsbury,
Bristol BS32 4SQ
GRANDE BRETAGNE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Decryption semiconductor circuit

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s)
revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04L9/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of
filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT SE SI SK TR LI

DECRYPTION SEMICONDUCTOR CIRCUIT

FIELD OF THE INVENTION

This invention relates to apparatus for securely selecting data pathways in an encryption or decryption system, and in particular to securely routing encryption or decryption keys in a pay-television system.

BACKGROUND OF THE INVENTION

The use of encryption techniques in subscriber based systems is essential to prevent unauthorised access to broadcasts by parties who are not entitled to them. For example, a person may wish to gain access to a sports broadcast service without making the appropriate payment to the broadcast service provider.

Many encryption techniques make use of secret electronic keys to encrypt broadcast data so that the data can only be comprehended when decrypted using a specified key possessed by a subscriber. In a typical system, various keys are provided for different encryption operations which need to be securely routed along with other data to or from various internal memories or other external sources or destinations.

We have appreciated that it is important to ensure that encryption or decryption keys and other confidential data are not intercepted otherwise the security of the system may be jeopardised. In prior software based systems, processors running computer programs are used to control data routing. Such systems are vulnerable to hacking when computer code is modified causing sensitive data to be routed to insecure data destinations where the hacker is able to obtain it. We have also appreciated the need for a means to securely control the routing of encryption keys.

SUMMARY OF THE INVENTION

The invention is defined in the independent claims to which reference may now be made. Advantageous features of 5 the invention are set forth in the dependant claims.

A system embodying the invention is a semiconductor integrated circuit comprising a plurality of encryption or decryption key stores, a plurality of data sources and destinations and a cryptographic circuit. The key stores, 10 data sources and destinations and the cryptographic circuit are inter-connected by a network of selectable data pathways to allow data to be routed from specific sources to specific destinations. In particular, encrypted or decrypted data is routed from one of the data sources to 15 the cryptographic circuit, an encryption or decryption key is routed from one of the key stores to the cryptographic circuit, and decrypted or encrypted data is routed from the cryptographic circuit to one of the data destinations or key stores. The data pathways may be securely selected 20 according to one or more predefined rules.

The data pathways are selected by setting the switching states of a plurality of routing components which mutually connect the plurality of data pathways and route data between selected pathways according to their switching 25 states. The switching states of the routing components are controlled by the output of an instruction interpreter which receives two input signals and combines them to generate the output control signal. The first input comprises a signal representative of an instruction to 30 select a data pathway appropriate for a particular encryption or decryption operation. The second input comprises a signal representative of a rule which defines those pathway configurations which are valid for a particular mode of operation of the system. In one embodiment the two inputs comprise bit fields which are 35

combined by a logic circuit to produce an output bit field. The logic circuit comprises a series of combinatorial components arranged so as to correctly interpret the instruction input according to the rule input. The output 5 signal sets the routing components to the appropriate switching states only if the instruction is valid as determined by the rule signal.

In one embodiment the second input signal is generated by a rule selector. The rule selector comprises 10 a series of anti-fuses or one time only switches which generates a bit field as an output. The series of anti-fuses are set to the appropriate state to generate a selected bit field output, and once set, remain in that state indefinitely. Each bit field combination corresponds 15 to a different rule selection scheme which defines the allowability of each pathway configuration. By setting the anti-fuses, a generic rule selector with many possible rule schemes may be tailored to a specific application depending on the particular rule set required for that application.

20 The instruction interpreter, rule selector, cryptographic circuit and data pathways are all contained on a single monolithic semiconductor integrated circuit to prevent unauthorised modification of the system and to increase security.

25

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a schematic diagram of a semiconductor circuit embodying the invention;
Figure 2 is a schematic diagram of an instruction signal;
Figure 3 is a schematic diagram of a series of anti-fuses
30 in the rule selector shown in Figure 1;
Figure 4 is a schematic diagram of a portion of the instruction interpreter shown in Figure 1.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The embodiment of the present invention relates to delivery of digital content such as music, video or games, but in particular to pay-television systems in which a subscriber may receive and view television broadcasts in return for payment of a subscription charge. Television broadcasts are received in a scrambled form to prevent unauthorised recipients from viewing the broadcast service. The subscriber may descramble the television broadcast using a decryption key to decrypt encrypted control words used to scramble the broadcast. In the preferred embodiment, different encryption or decryption keys may be used to encrypt or decrypt control words specific to different broadcast services. A subscriber possesses the decryption keys associated with those broadcast services to which he is entitled. When encryption or decryption keys are specific to particular broadcast services, they may be conveniently referred to as service keys or common keys.

To provide a plurality of service keys to subscribers, the service keys are transmitted over air and may be themselves encrypted in accordance with a secret key which is unique to a particular subscriber. This encryption prevents others from intercepting broadcasts and illegitimately obtaining the service keys. The plurality of service keys are transmitted to, and received by the subscriber encrypted in accordance with the secret key. The keys are decrypted and a service key may thereby be acquired. Performing the various operations described above requires controlled routing of various data around the system. Furthermore, since the purpose of the above described operations are to prevent unauthorised access to broadcasts, the routing of the data must be secure to maintain the integrity of the system.

Figure 1 is a schematic diagram of a semiconductor circuit for use in an encryption or decryption system such as a pay television system in which the invention is employed. The system comprises a plurality of memories or stores 1, 3, 5, 7 which each stores one or more keys which may be used to encrypt or decrypt digital data, a cryptographic circuit 9, here an AES circuit, to encrypt or decrypt digital data using encryption or decryption keys, and a plurality of data sources and destinations 11, 13, 15, 17, 19 from which data may be received or to which data may be transmitted, either encrypted or decrypted.

The key memories 1, 3, 5, 7 contain encryption or decryption keys which may be used in various encryption or decryption operations. An encryption or decryption key may be in the form of for example a 128 bit digital data packet. A first key memory 1 comprises a table containing one or more common or service keys used to decrypt control words used to scramble various broadcast services. A subscriber gains viewing rights to pay television services by virtue of his possession of the appropriate service keys. A second key memory 3 contains a secret key which is unique to a particular subscriber. This key may be used to encrypt or decrypt service keys and provides a means to prevent persons from obtaining service keys to which they are not entitled. A third key memory 5 comprises a table containing one or more written keys generated by a processor running a software algorithm. These keys may be used where large numbers of unique keys are required, for example in frequent memory to memory transfers. A forth key memory 7 comprises a table containing one or more secure keys, which may be derived from either the secret key or a written key by performing a transform algorithm, or combining with other keys or data. A further memory 8 comprises a table containing a plurality of control words used to scramble or descramble television broadcast data.

The integrity of the system relies on the confidentiality of these keys and data, so it is essential that they are not routed to destinations where they become available to hackers. It is therefore also essential that hackers are 5 prevented from modifying the system to allow unauthorised re-routing of data.

The data sources and destinations 11, 13, 15, 17, 19 provide encrypted or scrambled data to the system and may be used to store decrypted or descrambled data. A 'data in' 10 port 11 receives scrambled broadcast television signals, encrypted control words used to descramble the television signals, and encrypted keys used to decrypt the control words. A 'data out' port 13 transmits descrambled television signals from the system to a video display unit. 15 A hard disc drive 15 may be provided to act as a buffer or video recorder to store scrambled or descrambled broadcast data. The hard disc drive 15 may also be used to store data corresponding to a particular subscriber such as personal details, credit data, viewing rights and subscriber 20 selected settings. A read only memory (ROM) 17 is provided to store an operating system, error correction algorithms, system checking routines, encryption key generating algorithms and any other programs required for operation of the system. A random access memory (RAM) 19 is provided as 25 a temporary data store during operation of the system. A central processing unit (CPU) 21 is provided to control the system including controlling the flow of data around the system, and to execute programs stored on the ROM 17. For example, the CPU 21 may generate written keys using an algorithm stored on the ROM 17. Additionally, the key 30 memories may also be regarded as data sources or destinations. The ROM 17 and in port 11 are data sources only, the out port 13 is a data destination only, and the hard drive 15 and RAM 19 are both data sources and 35 destinations. Data sources and destinations external to the

circuit 39 may interface with the circuit 39 via input and output interfaces 20, 22. Some data sources and destinations are less secure than others. For example, a hacker has easy access to data ports while internal key 5 memories are more secure. Therefore, it is essential that confidential data such as decrypted keys are not illegally routed to vulnerable sources. For example, a hacker may attempt to circumvent the security of the system by re-routing the secret key to the out port.

10 The cryptographic circuit 9 comprises a circuit having inputs 24 and an output 26 arranged to encrypt or decrypt data using an encryption or decryption key retrieved from one of the key memories. The cryptographic circuit 9 receives as an input, data either in an encrypted 15 or unencrypted form from one or more of the data sources, an encryption or decryption key from one of the key memories, and encrypts or decrypts the data according to a specified algorithm. The data may be encrypted or decrypted by any appropriate encryption algorithm such as the 20 Advanced Encryption Standard (AES) algorithm or any other symmetric cryptographic transform. The purpose of encrypting data is so that unauthorised persons cannot gain access to the data. It is important therefore to maintain the security of the system so that keys are not acquired by 25 persons not entitled to them so that they can illegitimately decrypt broadcast signals. Encrypted or decrypted data is output from the cryptographic circuit 9 and may be sent to one or more data destination such as a display unit via the out port 13 or the hard disc 15.

30 The key memories, cryptographic circuit 9 and data sources and destinations are inter-connected by a network of selectable communication links or data pathways 23. The configuration of the data pathways 23 are determined by a plurality of routing and selection components such as 35 switches 25 and multiplexors (MUXs) 27. A switch 25 may be

set so that one input pathway is selectively connected to one of a plurality of output pathways according to the setting of the switch 25. A MUX 27 may be set so that one of a plurality of input pathways is selected as an output pathway according to the setting of the MUX 27. Data flows around the system along the pathways 23, and is selectively routed according to the switching states of the routing components connecting the pathways 23. For example, scrambled television signals may be selectively routed from the in port 13 to the cryptographic circuit 9, control words may be selectively routed from the control word memory 8 to the cryptographic circuit 9, and the resulting descrambled television data may be selectively routed from the cryptographic circuit 9 to the out port 13.

The routing components are controlled by an instruction interpreter 29 which outputs a plurality of control signals 31 each one representative of a switching state and which controls one of the plurality of routing components. In one embodiment, the selection between the plurality of data sources and destinations may be made directly by a MUX. Alternatively, a direct memory access (DMA) processor may be provided to deal with complex memory operations involving transfers of large blocks of data. In this case, the data sources and destinations interface via a data bus with the DMA. The DMA receives signals from the instruction interpreter 29 and CPU 21 to select between various data sources and destinations and to transfer data to or from them. The DMA then provides the data to the cryptographic circuit 9. The instruction interpreter 29 allows the DMA to define a memory address and block size for a data transfer rather than having to transfer each data word at a time, thereby improving data transfer efficiency. The instruction interpreter 29 receives two inputs which are combined to produce the output control signals 31 to control the switching states of the routing components.

The first input 33 of the instruction interpreter 29 comprises a signal representative of an instruction defining a data pathway configuration of the system. The first input, or instruction signal 33 is generated by the 5 CPU 21 and transmitted to the instruction interpreter 29 when an encryption or decryption operation is required. Figure 2 is a schematic diagram of an instruction signal. In the preferred embodiment, the instruction signal 33 comprises a 32 bit data field composed of two 16 bit 10 portions. The first portion 50 contains an instruction corresponding to a particular data pathway configuration of the system. For example, one instruction may correspond to a pathway configuration in which a broadcast encrypted service key, and the secret key are routed to the 15 cryptographic circuit 9, and the decrypted service key routed to the service key memory 1. Each bit of the first portion, or instruction portion 50 may correspond directly to the switching state of a particular routing component. Preferably, the instruction is in the form of an abstract 20 code which is representative of a pathway configuration according to a predetermined scheme. The second portion 52 may contain further data necessary to fully define the instruction. For example, if the instruction portion 50 corresponds to retrieving a block of data from a memory, 25 the second portion, or data portion 52 contains the start and end memory addresses of the data. Alternatively, the data portion 52 may contain data instructing the instruction interpreter 29 to expect receipt of further related instructions, for example from the CPU 21 or the 30 DMA processor. In this way, multi-word length instructions may be provided for. If an instruction 33 corresponds to an operation requiring a software written key, the data portion 52 may contain the key data generated by the CPU. 35 In this case the instruction portion 50 is input into the instruction interpreter 29 by the CPU 21 while the data portion 52 is separated and input via an alternative data

pathway, 23a of Figure 1, into the cryptographic circuit 9. In this way, the written key is used immediately rather than having to be stored in the key memory 5 first.

The second input 35 to the instruction interpreter 29 comprises a signal representative of a rule which defines those pathway configurations which are valid for a particular mode of operation of the system. For example, if encrypted data is received from a particular destination, the secret key only may be used to decrypt the data. The second input, or rule signal 35 is generated and output from a rule selector 37 and transmitted as an input to the instruction interpreter 29. The rule signal 35 comprises a bit field and is generated by a series of anti-fuses in the rule selector 37. Figure 3 is a schematic diagram of a series of anti-fuses in the rule selector shown in Figure 1. An anti-fuse 60 is a component which generates an electrical signal of 0 or 1 units depending on how the anti-fuse 60 is configured, and once configured initially, the anti-fuse 60 remains in that state indefinitely. In this way a permanent, selectable bit field may be generated. Such anti-fuses are known to those skilled in the art. Alternatively, the rule signal 35 may be generated by a non volatile or 'write once' memory or software writer.

The instruction interpreter 29 comprises a logic circuit containing a series of combinatorial components. Figure 4 is a schematic diagram of a portion of the instruction interpreter shown in Figure 1. Instruction signal input 33 comprises a bit field which includes individual bit signals 80, 82, and rule signal input 35 comprises a bit field which includes individual bit signals 84, 86. The input signals are input into two AND gates 88, 90 such that input signals 80 and 84 are input into AND gate 88, and input signals 82 and 86 are input into AND gate 90. Output control signal 31 comprises a bit field including individual bit signals 92 and 94. Output bit

signal 92 corresponds to the output of AND gate 88, and output bit signal 94 corresponds to the output of AND gate 90. Each input and output bit signal may take one of the values 1 or 0 and the output of each AND gate is 1 if both inputs are equal to 1, otherwise the output of the AND gate is 0. If the rule signal input is set such that both bit signals 84 and 86 are set to 1, then the outputs 92 and 94 correspond to the inputs 80 and 82 respectively. In this case, the output signals 92, 94 are controllable by input signals 80, 82. If however, rule input bit signal 84 is set to 0, then output bit signal 92 is always 0. Setting rule input bit signal 84 to 0 thus prevents instruction input signal 33 from setting output 92. Output 94 remains controllable by input 82. The switching state of the routing component controlled by output bit signal 92 is restricted, even if a hacker intercepts and alters or replaces the instruction signal 33. Similarly, setting rule input bit signal 86 to 0 prevents instruction input signal 33 from setting output 94. It is understood that the configuration of combinatorial components within the instruction interpreter 29 may be much more complicated than the exemplary configuration shown in Figure 4. For example, the instruction interpreter may contain other logic components arranged so as to generate an control signal output 31 as a logical function of the instruction signal input 33 and rule signal input 35.

The role of the rule selector 37 may now be seen more clearly. The rule selector 37 acts to block or select which instructions 33 input into the instruction interpreter 29 are able to influence the switching state of some or all of the routing components. In this way, pathway configurations which route confidential data to vulnerable data destinations are blocked, whatever instruction 33 is input into the instruction interpreter 29. In this way, even if a hacker is able to feed selected instructions 33 into the instruction interpreter 29, the rule selector 37

ensures that only secure data pathways are allowed according to a set of predefined rules. The set of rules are determined by the precise rule signal 35 generated by the rule selector 37.

5 In one embodiment, the instruction interpreter 29 further comprises timing means to allow more sophisticated sequences of operations to be carried out dynamically. In this case the instruction signal 33 may contain timing information so that several encryption or decryption
10 operations may be carried out in a defined order or at certain times. For example, a routing component may need to be switched during a data transfer. In one embodiment, the instruction signal 33 and rule signal 35 are combined by the instruction interpreter 29 by means of a micro
15 controller instead of, or in addition to a logic circuit. In this embodiment, the instruction signal 33 or rule signal 35 may be used as an index to a look-up table to retrieve the appropriate pathway configuration and generate an output control signal accordingly. Alternatively, the
20 micro controller may execute an algorithm to determine the appropriate output signals. In one embodiment, the rule selector and instruction interpreter are combined in a single component. In this case, the instruction interpreter does not receive an external rule signal, but instead, the
25 means by which rules are defined are created within the instruction interpreter.

The instruction interpreter 29, rule selector 37, cryptographic circuit 9, key memories 1, 3, 5, 7, 8, CPU
30 21 and data pathways 23 are all contained on a single monolithic semiconductor integrated circuit 39. This increases the integrity of the system since data cannot easily be intercepted from within the system and components cannot easily be substituted with illegitimate replacements to attempt to circumvent security. Advantageously, the
35 control of the routing components and hence the data flow within the system is controlled by the hardware based

instruction interpreter 29. Unlike software based controllers in which software can be modified by hackers, hardware is more secure and less prone to tampering. As an additional level of security, the rule selector 37 ensures 5 that even if a hacker is able to infiltrate the system and feed illegitimate instructions into the instruction interpreter 29, these instructions are blocked and security is maintained.

The anti-fuses in the rule selector 37 are configured 10 to generate a rule signal 35 corresponding to those data pathways which are valid for a particular mode of operation of the system. One particular application or mode of operation will allow certain procedures that are illegal 15 in other applications. Initially, the rule selector 37 has the potential to select rules according to a number of applications or rule selection schemes. The anti-fuses are then configured to generate a specific rule signal output 35 and the system becomes tailored permanently to one specific application. In this way, many different systems 20 may be constructed using the same hardware reducing manufacturing and design costs.

In one embodiment, the rules defining allowed procedures may be any of the following:

1. Only use the secret key for decrypting service keys.
2. Use software written keys for memory to memory transfers.
3. Only use secure keys for memory transfers.
4. Only use service keys for decrypting control words.
5. Use software written keys for decryption operations.
- 30 6. Use a source identification for all data transfers and permit or reject the data transfer according to the identification of the source and the destination.

When an instruction 33 is input into the instruction interpreter 29, the instruction interpreter 29 combines the

instruction 33 with the rule signal 35 generated from the rule selector 37. If the instruction is compatible with a chosen rule, for example one or more of the above rules, then the control signal 31 output causes the routing
5 components to switch to the appropriate switching states. If however the instruction interpreter 29 receives an instruction 33 representing an unallowed process, the influence of the rule signal 35 ensures that the instruction 33 is blocked and no output control signals 31 are generated. For example, in the first case above, an instruction 33 to decrypt a service key using a written key would be blocked. In another application, however, this procedure may be allowed and the rule signal 35 would be generated such that this instruction would not be blocked.
10 Rules 2 and 3 above may be used as alternatives to each other. In the last case above, an instruction 33 to perform a data transfer contains information in the data portion 52 of the instruction signal 33 identifying the data source and destination of the transfer. The rule signal ensures
15 that the data transfer is only allowed if the data source and destination are one of an allowed combination as defined by the rule signal 35.
20

CLAIMS

1. A semiconductor integrated circuit (39) comprising:
 - a plurality of selectable pathways (23) interconnected between a plurality of data sources and data destinations (11, 13, 15, 17, 19);
 - a cryptographic circuit (9) connected to the selectable pathways (23) and arranged to selectively receive data at an input (24) from at least one of the data sources, to decrypt or encrypt the data in accordance with a key, and selectively provide the encrypted or decrypted data to at least one of the data destinations via an output (26);
 - an instruction interpreter (29) arranged to receive as an input an instruction signal (33) and to generate therefrom an output (31) to control the plurality of selectable pathways (23) to select from which of the data sources the cryptographic circuit (9) receives data and to which destination the cryptographic circuit (9) provides data;

the instruction interpreter (29) being configured such that the instruction signal (33) defines a data pathway configuration of the system, and such that it operates in accordance with a rule which limits the data pathway configurations which are selectable.
2. A semiconductor integrated circuit according to claim 1, wherein the instruction interpreter (29) is arranged to receive a rule signal (35) defining those data pathway configurations which are unselectable.

3. A semiconductor integrated circuit according to claim 2, wherein the rule signal (35) is chosen from a plurality of possible rule signals according to a mode of operation of the system.
4. A semiconductor integrated circuit according to claim 3, wherein the rule signal (35) is generated by a rule selector (37), and wherein the rule selector (37) comprises a plurality of anti-fuses (60) allowing one of a plurality of selectable configurations to be chosen.
5. A semiconductor integrated circuit according to claim 4, wherein each of the anti-fuses (60) can be configured once only.
6. A semiconductor integrated circuit according to any preceding claim, wherein the instruction signal is generated by a CPU (21).
7. A semiconductor integrated circuit according to claim 6, wherein the CPU (21) is arranged to generate an instruction signal (33) comprising an instruction portion (50) and a data portion (52).
8. A semiconductor integrated circuit according to any preceding claim, wherein the instruction signal (33) and rule signal (35) are 32 bit data fields.
9. A semiconductor integrated circuit according to any preceding claim, wherein the plurality of data sources and destinations includes at least one memory for storing encryption or decryption keys (1, 3, 5, 7, 8).

10. A semiconductor integrated circuit according to any preceding claim, wherein the key is selected from a plurality of keys in dependence on the instruction signal (33).
- 5 11. A semiconductor integrated circuit according to claim 10, wherein the key is selected from one of a plurality of key stores and provided to a key input (24) of the cryptographic circuit (9) in dependence on the instruction signal (33).
- 10 12. A semiconductor integrated circuit according to claim 10 or 11, wherein the cryptographic circuit (9) has a key input (24), and the key provided to the key input (24) is selected in accordance with the selected pathway.
- 15 13. A semiconductor integrated circuit according to any preceding claim, wherein the circuit (39) is arranged to descramble television broadcast signals using a series of control words.
- 20 14. A semiconductor integrated circuit according to any preceding claim, wherein the circuit (39) is arranged to decrypt encrypted control words using a service key.
- 25 15. A semiconductor integrated circuit according to any preceding claim, wherein the circuit (39) is arranged to decrypt encrypted service keys using a secret key.
16. A semiconductor integrated circuit according to any preceding claim, wherein the circuit (39) is arranged to perform memory to memory transfers.

17. A semiconductor integrated circuit according to claim 12, wherein the plurality of selectable pathways (23) are configurable such that when the data from the data source is a service key, the cryptographic circuit (9) receives a secret key at the key input (24).
5
18. A semiconductor integrated circuit according to claim 12, wherein the plurality of selectable pathways are configurable such that when the data source is a memory and the data destination is a memory, the cryptographic circuit (9) receives a software written key at the key input (24).
10
19. A semiconductor integrated circuit according to claim 12, wherein the plurality of selectable pathways are configurable such that when the data source is a plurality of control words, the cryptographic circuit (9) receives a service key at the key input (24).
15
20. A semiconductor integrated circuit according to claim 12, wherein the plurality of selectable pathways are configurable such that when the data source is broadcast data, the cryptographic circuit (9) receives a software written key at the key input (24).
20
21. A semiconductor integrated circuit according to claim 9, wherein one of the key memories (5) stores at least one key generated by a software algorithm.
25
22. A semiconductor integrated circuit according to claim 9, wherein one of the key memories (1) stores at least one service key for decrypting control words.

23. A semiconductor integrated circuit according to claim 9, wherein one of the key memories (3) stores a secret key for decrypting service keys.
24. A semiconductor integrated circuit according to any preceding claim, wherein the plurality of data sources and destinations includes at least one of a hard disc, ROM, RAM, data in port and data out port.
5
25. A semiconductor integrated circuit according to any preceding claim, wherein the cryptographic circuit (9) is an AES circuit.
10
26. A semiconductor integrated circuit according to any preceding claim, wherein the plurality of selectable pathways (23) are selected by at least one multiplexor (27) or switch (25).
15
27. A semiconductor integrated circuit according to any preceding claim, wherein the instruction interpreter (29) comprises a plurality of combinatorial components arranged such that the output (31) is generated as a function of the instruction signal (33).
20
28. A semiconductor integrated circuit according to any preceding claim, wherein the encryption system is a subscriber based pay-television system.
29. A semiconductor integrated circuit according to any preceding claim, wherein the encryption system is a monolithic integrated circuit (39).
25
30. A method of configuring a circuit (37) for selecting routing rules in an encryption system comprising configuring one or more of a plurality of anti-fuses

(60) within the circuit (37) such that the circuit (37) is configured to select routing rules according to a rule selection scheme, wherein the rule selection scheme depends upon the configuration of the circuit (37) and wherein each of the anti-fuses (60) can be configured once only.

ABSTRACT

A semiconductor integrated circuit (39) comprising: a plurality of selectable pathways (23) inter-connected between a plurality of data sources and data destinations (11, 13, 15, 17, 19); a cryptographic circuit (9) connected to the selectable pathways (23) and arranged to selectively receive data at an input (24) from at least one of the data sources, to decrypt or encrypt the data in accordance with a key, and selectively provide the encrypted or decrypted data to at least one of the data destinations via an output (26); an instruction interpreter (29) arranged to receive as an input an instruction signal (33) and to generate therefrom an output (31) to control the plurality of selectable pathways (23) to select from which of the data sources the cryptographic circuit (9) receives data and to which destination the cryptographic circuit (9) provides data; the instruction interpreter (29) being configured such that the instruction signal (33) defines a data pathway configuration of the system, and such that it operates in accordance with a rule which limits the data pathway configurations which are selectable. Preferably, the instruction interpreter (29), cryptographic circuit (9) and data pathways (23) are all contained on a single monolithic semiconductor integrated circuit (39).

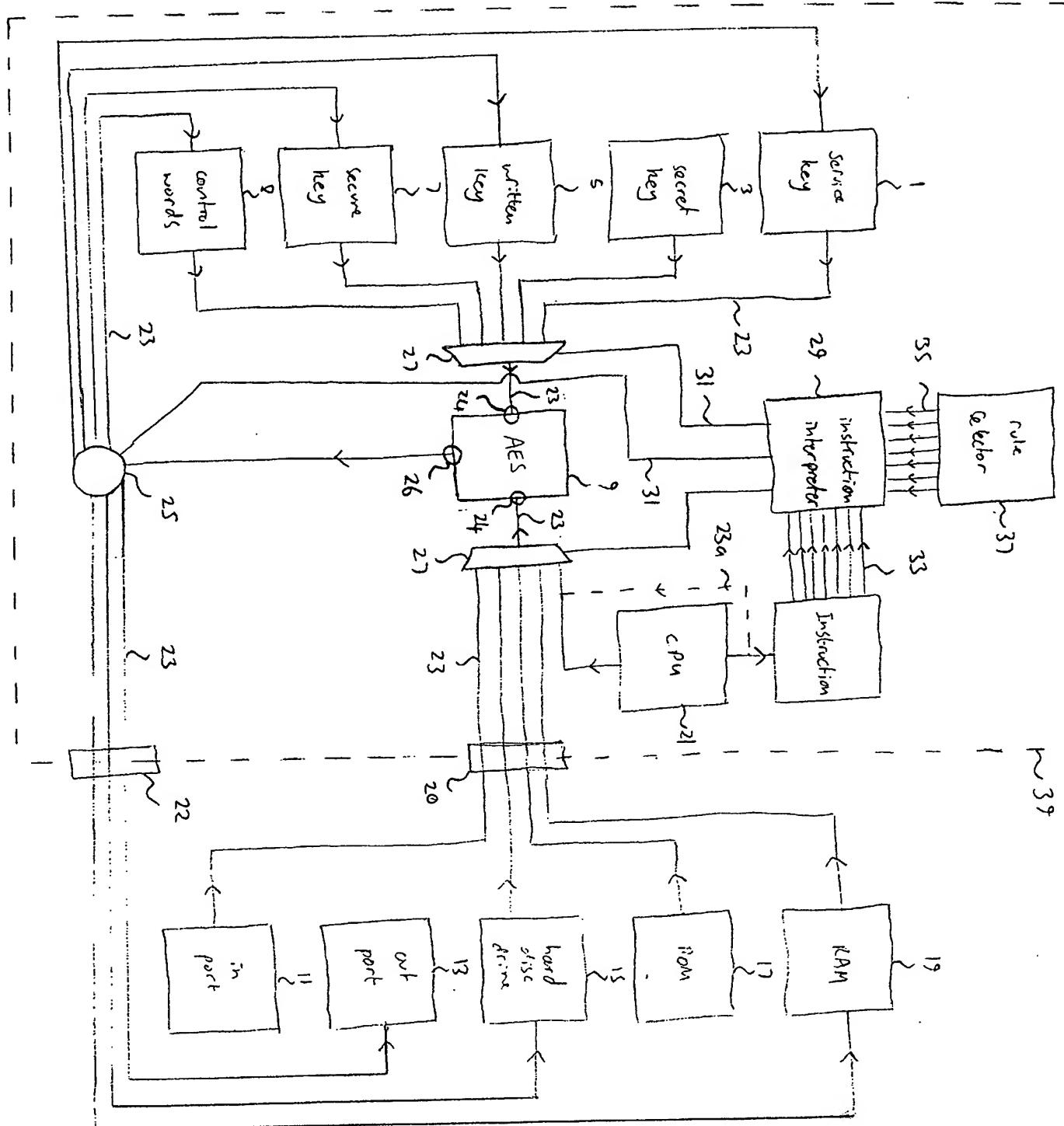
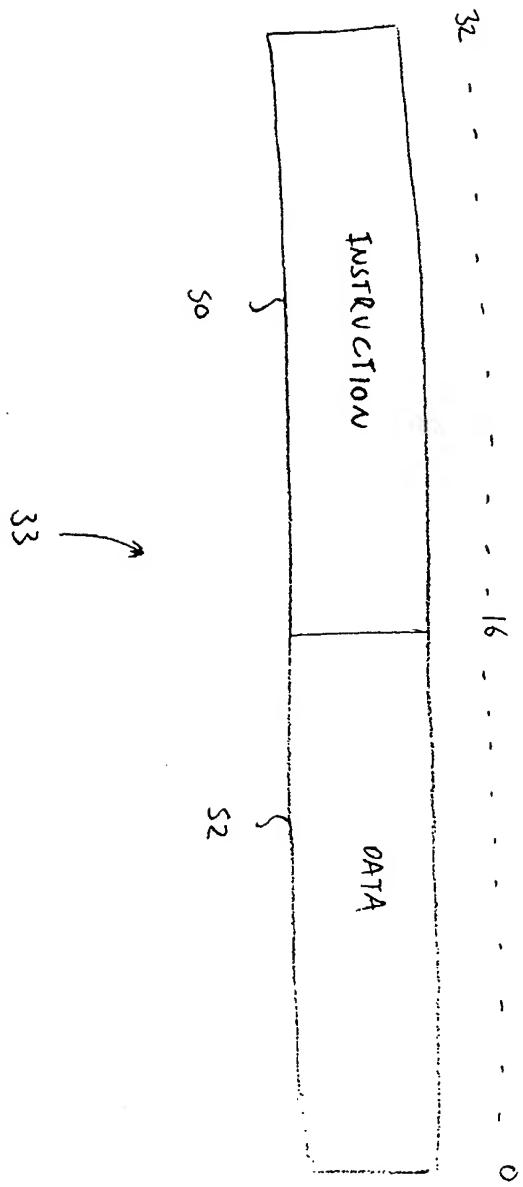


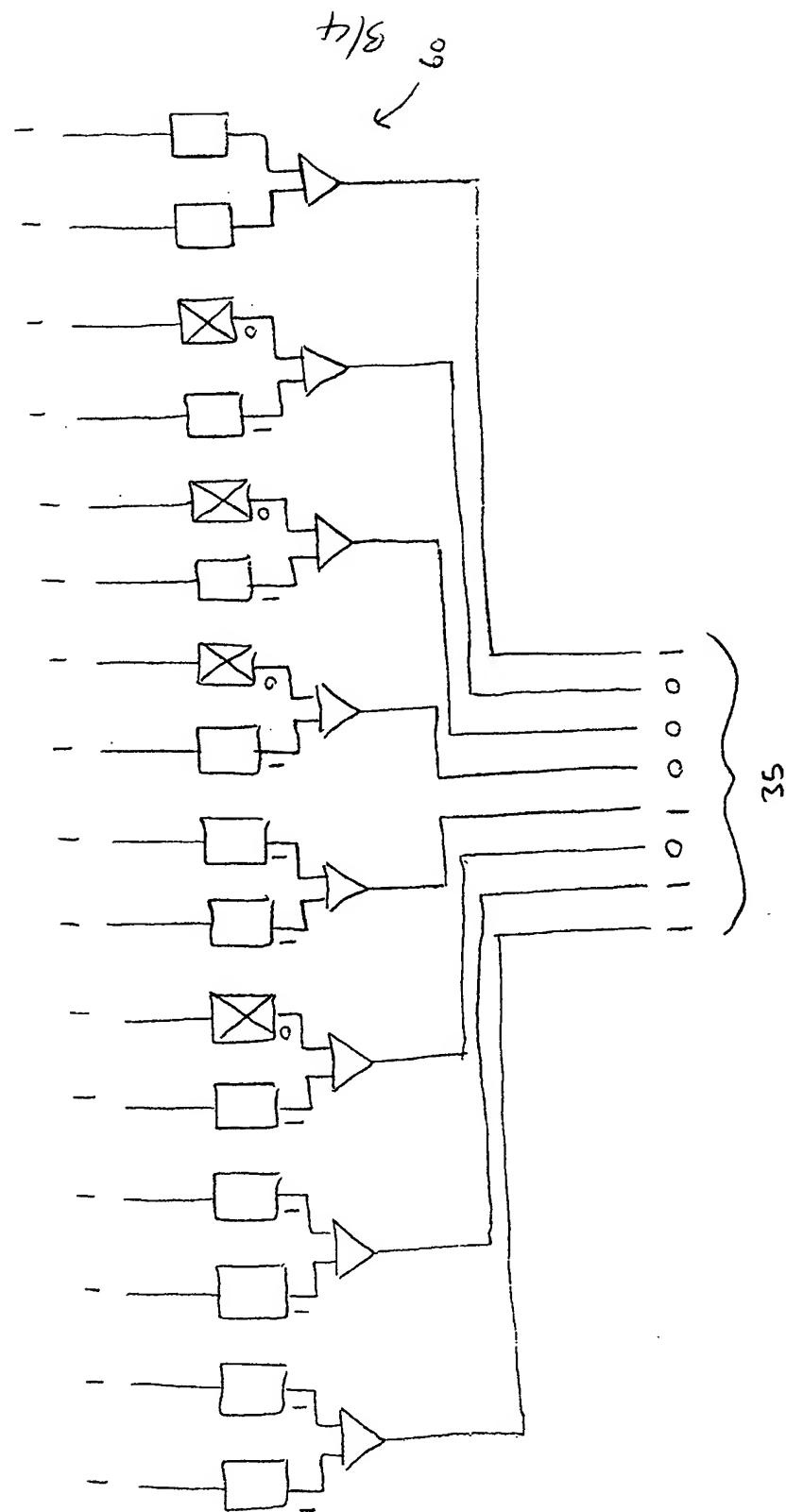
Figure 1

Figure 2



214

Figure 3



29

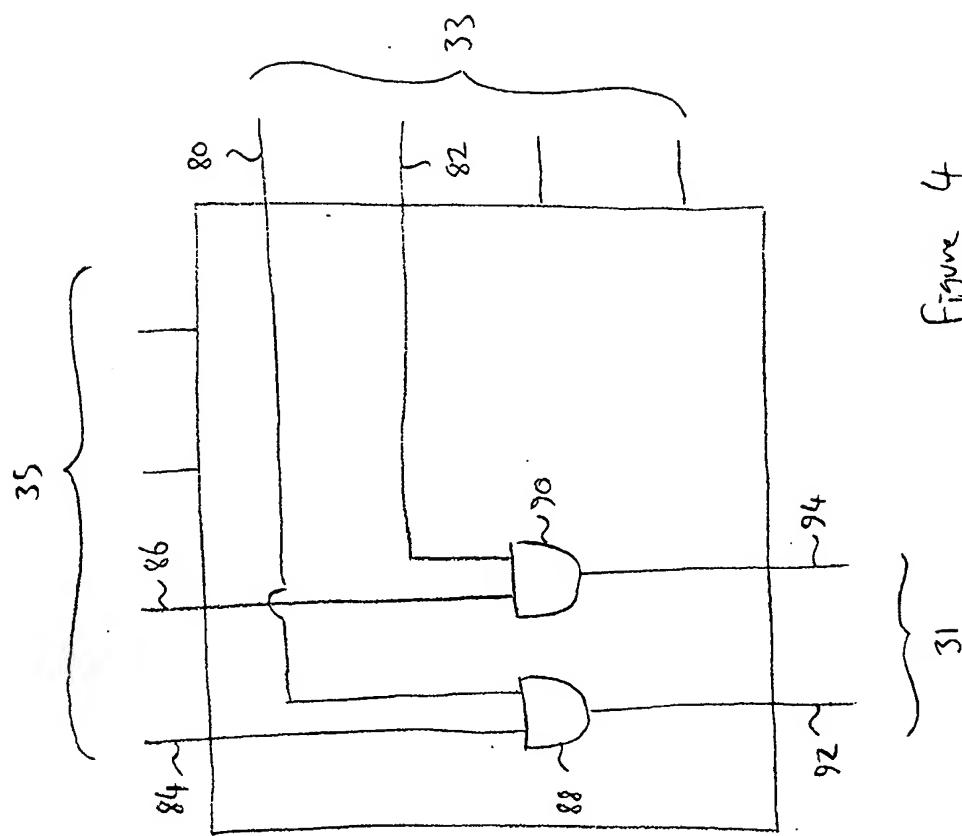


Figure 4